



**Bojíte se?
Poříd'te si**



Petr Řehoř, ICZ a.s.
4. dubna 2011

Agenda

- ▶ **Bojíte se? Poříd'te si Intel® Anti-Theft!**
- ▶ **Jak Intel® Anti-Theft funguje?**
- ▶ **Jak si Intel® Anti-Theft pořídít?**

Bojíte se?

Bojíte se, že přijdete o svůj notebook a o data, která na něm máte uložená?

Poříd'te si Intel® Anti-Theft!

Technologie Intel® Anti-Theft integrovaná do notebooků nabízí možnost zablokovat ukradený notebook a zabránit v přístupu k datům uloženým na pevném disku.

Elegantní mladík krade notebooky po firmách, policii zatím uniká

1. listopadu 2010 14:28

PRAHA - Pohledný, slušně oblečený mladík vejde do budovy, prohodí pár slov s recepční a vejde do kanceláří. Z nich si vždy odnáší několik notebooků. Takový je scénář krádeží, které se staly v pěti pražských firmách. Po elegantním zloději policie nyní pátrá.

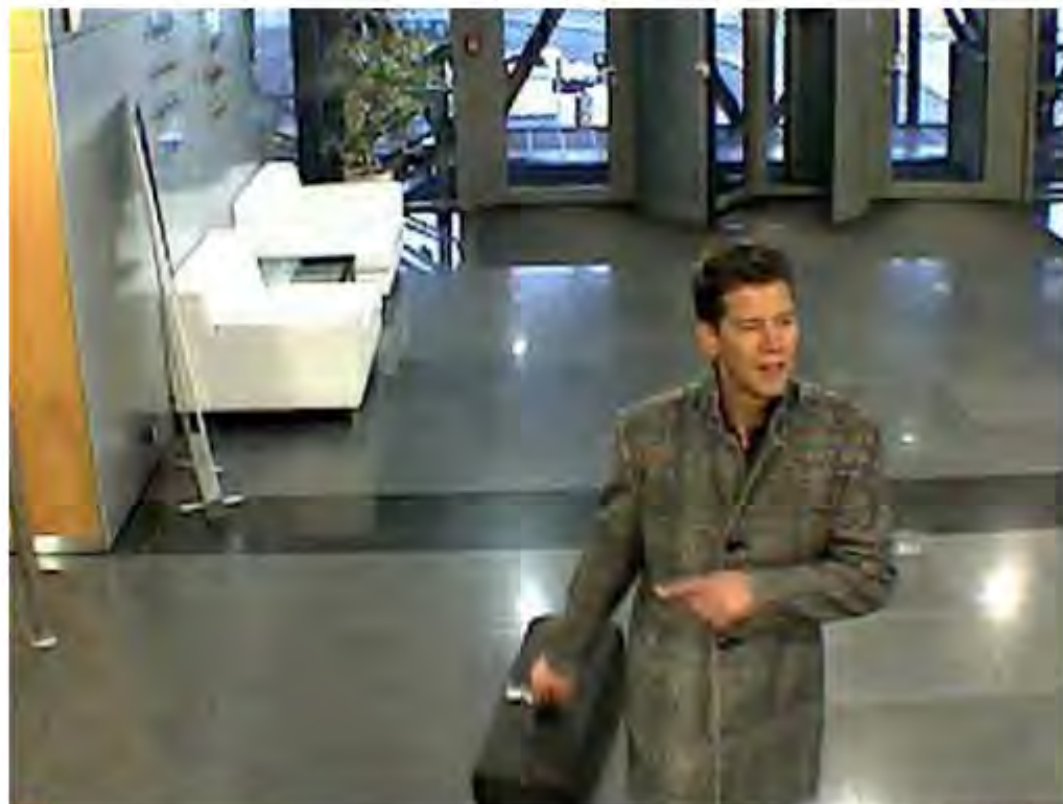
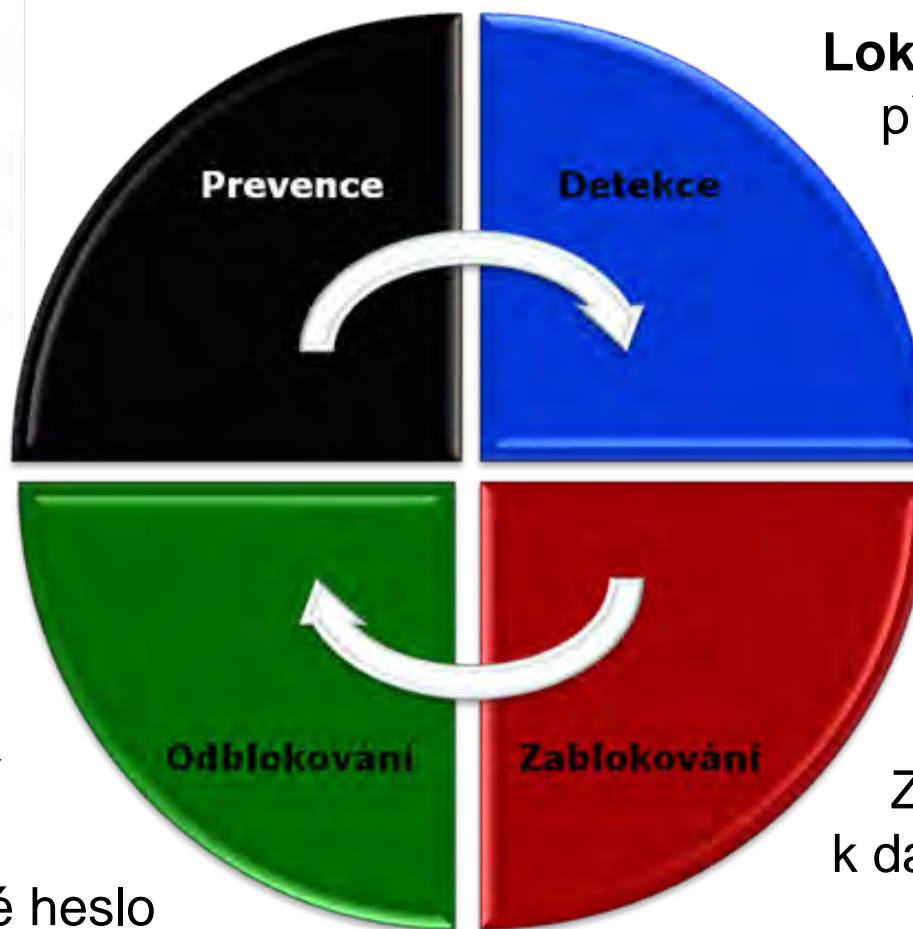


foto: Policie ČR.

"Muž od začátku července z kanceláří různých společností na [Praze 3](#) a [Praze 8](#) odcizil větší množství notebooků," sdělila serveru Lidovky.cz policejní mluvčí Eva Kropáčová.

Jak Intel® Anti-Theft funguje?



Lokální: neúspěšná přihlášení, časovač

Vzdálená: Internet, SMS

Není možné nastartovat OS

Zabránění přístupu k datům na disku

Návod jak počítač odblokovat

Lokální: lokální heslo pro odblokování

Vzdálené: jednorázové heslo pro odblokování

Prevence

- ▶ Notebook je označen výrazným logem technologie Intel® Anti-Theft



intel® **ANTI-THEFT**
TECHNOLOGY

Detekce

▶ Neúspěšná přihlášení

- Anti-Theft sleduje počet neúspěšných přihlášení do BIOSu při startu počítače. Při překročení povoleného počtu neúspěšných přihlášení se notebook zablokuje.

▶ Časovač

- Notebook se musí pravidelně spojit s řídicím serverem. Při překročení maximální povolené doby od posledního spojení se notebook zablokuje.

▶ Internet

- Uživatelem nahlášená ztráta nebo krádež notebooku je zaznamenána v řídicím serveru. Notebook se po připojení k řídicímu serveru zablokuje.

▶ SMS

- Řídicí centrum odešle speciální SMS notebooku a ten se zablokuje.

Zablokování

▶ **Není možné nastartovat OS**

- Notebook v zablokovaném stavu zobrazuje pouze obrazovku pro odblokování a není možné spustit operační systém.

▶ **Návod jak počítač odblokovat**

- Obrazovka pro odblokování notebooku může obsahovat informace pro uživatele jak při odblokování postupovat. Například telefonní číslo na HelpDesk.

▶ **Zabránění přístupu k datům na disku**

- Klíče pro šifrování souborů nebo disku, která jsou uložena v čipsetu mohou být smazána nebo skryta.

Odblokování

▶ Lokální heslo

- Obrazovka pro odblokování notebooku může umožnit zadat heslo, které si nastavil uživatel. Toto heslo je stále platné.

▶ Jednorázové heslo

- HelpDesk může uživateli sdělit nebo poslat formou SMS jednorázové heslo pro odblokování notebooku.

Pod kapotou

▶ Čipset

- Intel® Management Engine – servisní procesor pro Anti-Theft, Advanced Management Technology a vPro
- Umožňuje uložit šifrovací klíče pro šifrování disku

▶ BIOS

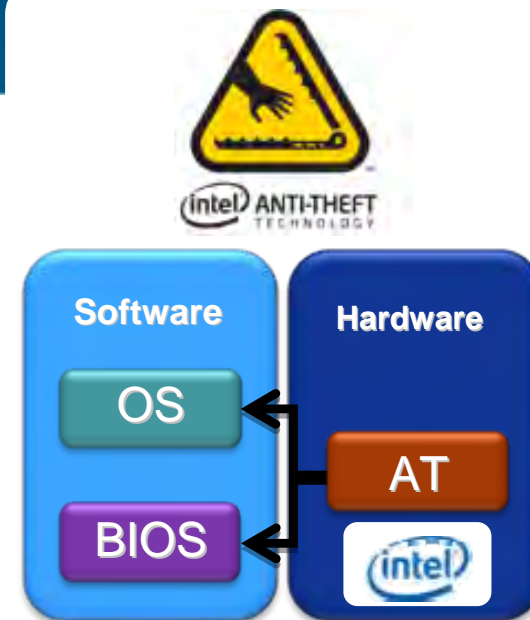
- Umožňuje konfiguraci Management Engine, podle stavu Anti-Theft zablokuje start OS a zobrazí obrazovku pro odblokování, podpora pro softwarového agenta

▶ Softwarový agent

- Komunikuje s řídicím serverem, poskytuje mu informace o stavu notebooku, na jeho požadavek notebook zablokuje

▶ Theft Management Server

- Řídicí server, ve kterém je notebook zaregistrován, vyhodnocuje údaje z notebooku



Pod kapotou

► Šifrování dat

- Softwarové šifrování souborů
- Softwarové šifrování disku
- Hardwarové šifrování disku (OPAL)

- Šifrování dat musí spolupracovat s Intel® Anti-Theft – ukládat si do něj šifrovací klíče. Potom je možné při zablokování notebooku tyto klíče zablokovat nebo smazat
- Pouze hardwarové šifrování disků nemá zásadní dopad na výkonnost diskových operací. U softwarového šifrování souborů nebo disků je potřeba počítat se snížením výkonu v řádu několika desítek procent

Jak si Intel® Anti-Theft pořídit

- ▶ **Portál technologie Intel® Anti-Theft**
 - Přehled notebooků obsahujících technologii Intel® Anti-Theft Technology
 - Přehled služeb využívajících technologii Intel® Anti-Theft

<http://antitheft.intel.com>

Služby pro Intel® Anti-Theft

▶ Absolute Computrace

- Pokročilé sledování notebooku formou služby
 - Geolokace - možnost omezit území na kterém se notebook používá
 - Pátrání v případě ztráty nebo zcizení
 - Garance vrácení notebooku nebo peněz
- Správa pomocí Microsoft System Center Configuration Manager
- Podporuje i Symbian S60, Windows Mobile a Blackberry

▶ Absolute Secure Drive

- Hardwarového šifrování disků (OPAL)
- Spolupráce s Computrace
 - Správa pomocí Active Directory

Služby pro Intel® Anti-Theft

▶ WinMagic SecureDoc

- Primárně zaměřeno na šifrování dat
- Softwarové i hardwarové šifrování celého disku
- Vlastní řídicí server SecureDoc Enterprise Server
- Umožňuje spolupráci s Absolute Computrace

▶ Symantec PGP Whole Disk Encryption

- Primárně zaměřeno na šifrování dat
- Softwarové i hardwarové šifrování celého disku
- Spolupráce s Intel Anti-Theft pomocí PGP Remote Disable & Destroy
- Vlastní řídicí server PGP Universal Server

Děkuji za vaši pozornost

Petr Řehoř
petr.rehor@i.cz
+420 737 280 114

ICZ a.s.
Sekce Bezpečnost
www.i.cz